4

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/517,480	12/07/2004	Albert Maria Arnold Rijckaert	NL 020494	6115

24737 7590 06/07/2007
PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
LOUIE, OSCAR A	
ART UNIT	PAPER NUMBER
2136	
MAIL DATE	DELIVERY MODE
06/07/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/517,480	**Applicant(s)** RIJCKAERT ET AL.	
	Examiner Oscar A. Louie	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 April 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

This final action is in response to the amendment filed on 04/04/2007. Claims 1-8 are pending and have been considered as follows.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-4 are rejected under 35 U.S.C. 102(b) as being anticipated by Blatter (US-5754651-A).

Claim 1:

Blatter discloses,

- "storing the stream of encrypted data;" "storing items with decryption information from the stream of messages" (i.e. "In response to control signal C, mux 37 selects either, the transport stream from unit 35, or in a playback mode, a datastream retrieved from storage device 90 via store interface 95. In normal, non-playback operation, the data packets comprising the program that the user selected to view are identified by their PIDs by selection unit 45. If an encryption indicator in the header data of the selected program packets indicates the packets are encryption, unit 45 provides the packets to decryption unit 50. Otherwise unit 45 provides non-encrypted packets to transport decoder 55. Similarly, the data packets comprising the programs that the user selected for storage are identified by their PIDs by selection unit 47. Unit 47 provides encrypted packets to decryption unit 50 or non-encrypted packets to mux 110 based on the packet header encryption indicator information.") [column 4 lines 44-58].

- "storing synchronization information linking respective points in the stored stream of encrypted data to respective ones of the items with decryption information" (i.e. "Program Clock References (PCRs) that permit synchronization and decoding of content packets. Upon detection of a timing information packet, that is a packet containing an adaptation field, decoder 55 signals controller 115, via an interrupt mechanism by setting a system interrupt, that the packet has been received. In addition, decoder 55 changes the timing packet destination flag in unit 65 and provides the packet to unit 60. By changing the unit 65 destination flag, unit 65 diverts the timing information packet provided by decoder 55 to the unit 60 buffer location assigned to hold data for use by controller 115, instead of an application buffer location.

  Upon receiving the system interrupt set by decoder 55, controller 115 reads the timing information and PCR value and stores it in internal memory") [column 5 lines 64-67 & column 6 lines 1-11].

- "replaying stored part of the stream of encrypted data in an abnormal temporal pattern" (i.e. "In recovering a program from a storage medium, a problem occurs if a playback device incorrectly applies the CPSI of a different program. The use of the incorrect CPSI data such as the PMT, may result in erroneous identification and assembly of data packets in the recovery of the program content and produce invalid data for display or processing, for example. This problem may arise, for instance, if a playback device does not apply the CPSI of the recovered program or does not recognize that the CPSI has changed and continues to apply the CPSI previously derived for a different program. The likelihood that this may occur is increased if the storage medium contains more than one program. In that case a playback device may cross program boundaries during a trick play or search operation, for example, and continue to apply the CPSI of the previous program. In order to alleviate the problem of applying incorrect CPSI parameters across program boundaries, controller 115 formats the CPSI in step 340 by employing the process of FIG. 4") [column 10 lines 52-67 & column 11 lines 1-3].

- "retrieving the items with decryption information for the points in said stored part during said replaying" (i.e. "In response to control signal C, mux 37 selects either, the transport stream from unit 35, or in a playback mode, a datastream retrieved from storage device 90 via store interface 95. In normal, non-playback operation, the data packets comprising the program that the user selected to view are identified by their PIDs by selection unit 45. If an encryption indicator in the header data of the selected program packets indicates the packets are encryption, unit 45 provides the packets to decryption unit 50. Otherwise unit 45 provides non-encrypted packets to transport decoder 55. Similarly, the data packets comprising the programs that the user selected for storage are identified by their PIDs by selection unit 47. Unit 47 provides encrypted packets to decryption unit 50 or non-encrypted packets to mux 110 based on the packet header encryption indicator information") [column 4 lines 44-58].

- "combining the retrieved items with decryption information with the stream during replay at times selected under control of the synchronization information" (i.e. "In response to control signal C, mux 37 selects either, the transport stream from unit 35, or in a playback mode, a datastream retrieved from storage device 90 via store interface 95. In normal, non-playback operation, the data packets comprising the program that the user selected to view are identified by their PIDs by selection unit 45. If an encryption indicator in the header data of the selected program packets indicates the packets are encryption, unit 45 provides the packets to decryption unit 50. Otherwise unit 45 provides non-encrypted packets to transport decoder 55. Similarly, the data packets comprising the programs that the user selected for storage are identified by their PIDs by selection unit 47. Unit 47 provides encrypted packets to decryption unit 50 or non-encrypted packets to mux 110 based on the packet header encryption indicator information") [column 4 lines 44-58].

Claim 2:

<u>Blatter</u> discloses,

- "subsampling messages from said stream of messages, only items with decryption information from subsampled ones of the messages being stored" (i.e. "Packets received by decoder 55 from units 45 and 50 that contain program content including audio, video, caption, and other information, are directed by unit 65 from decoder 55 to the designated application device buffers in packet buffer 60. Application control unit 70 sequentially retrieves the audio, video, caption and other data from the designated buffers in buffer 60 and provides the data to corresponding application devices 75, 80 and 85. The application devices comprise audio and video decoders 80 and 85 and high speed data port 75. Data port 75 may be used to provide high speed data such as computer programs, for example to a computer. Alternatively port 75 may be used to output data to an HDTV decoder, for example") [column 6 lines 23-35].

- "the synchronization information linking groups of points in the stored stream of encrypted data to respective ones of the subsampled items" (i.e. "Program Clock References (PCRs) that permit synchronization and decoding of content packets. Upon detection of a timing information packet, that is a packet containing an adaptation field, decoder 55 signals controller 115, via an interrupt mechanism by setting a system interrupt, that the packet has been received. In addition, decoder 55 changes the timing packet destination flag in unit 65 and provides the packet to unit 60. By changing the unit 65 destination flag, unit 65 diverts the timing information packet provided by decoder 55 to the unit 60 buffer location assigned to hold data for use by controller 115, instead of an application buffer location.

  Upon receiving the system interrupt set by decoder 55, controller 115 reads the timing information and PCR value and stores it in internal memory") [column 5 lines 64-67 & column 6 lines 1-11].

Claim 3:

Blatter discloses,

- "detecting a transition after which the messages contain decryption information different from decryption information in messages before transition" (i.e. "Units 45 and 47 employ PID detection filters that match the PIDs of incoming packets provided by mux 37 with PID values pre-loaded in control registers within units 45 and 47 by controller 115. The pre-loaded PIDs are used in units 47 and 45 to identify the data packets that are to be stored and the data packets that are to be decoded for use in providing a video image. The pre-loaded PIDs are stored in look-up tables in units 45 and 47. The PID look-up tables are memory mapped to encryption key tables in units 45 and 47 that associate encryption keys with each pre-loaded PID. The memory mapped PID and encryption key look-up tables permit units 45 and 47 to match encrypted packets containing a pre-loaded PID with associated encryption keys that permit their decryption. Non-encrypted packets do not have associated encryption keys. Units 45 and 47 provide both identified packets and their associated encryption keys to decryptor 50. The PID look-up table in unit 45 is also memory mapped to a destination table that matches packets containing pre-loaded PIDs with corresponding destination buffer locations in packet buffer 60. The encryption keys and destination buffer location addresses associated with the programs selected by a user for viewing or storage are pre-loaded into units 45 and 47 along with the assigned PIDs by controller 115. The encryption keys are generated by ISO 7816-3 compliant smart card system 130 from encryption codes extracted from the input datastream. The generation of the encryption keys is subject to customer entitlement determined from coded information pre-stored on the insertable smart card itself (International Standards Organization document ISO 7816-3 of 1989 defines the interface and signal structures for a smart card system)") [column 4 lines 59-67 & column 5 lines 1-22].

- "subsampling at least one of the subsampled messages at a predetermined position relative to the transition" (i.e. "Packets received by decoder 55 from units 45 and 50 that contain program content including audio, video, caption, and other information, are directed by unit 65 from decoder 55 to the designated application device buffers in packet buffer 60. Application control unit 70 sequentially retrieves the audio, video, caption and other data from the designated buffers in buffer 60 and provides the data to corresponding application devices 75, 80 and 85. The application devices comprise audio and video decoders 80 and 85 and high speed data port 75. Data port 75 may be used to provide high speed data such as computer programs, for example to a computer. Alternatively port 75 may be used to output data to an HDTV decoder, for example") [column 6 lines 23-35].

Claim 4:

Blatter discloses,

- "constructing a list of data pointers to selected parts of the stream of encrypted data, each data pointer being associated with a selected one of the items of decryption information that enables decryption of the encrypted data pointed at by the pointer" (i.e. "The PSI as defined in MPEG systems standard section 2.4.4 comprises four non-encrypted elements or tables of information. These are the Program Association Table (PAT), the Program Map Table (PMT), the Network Information Table (NIT) and the Conditional Access Table (CAT). Each table is formed from data packets that are recognized by a particular PID. The PMT defines the PID labels that identify the individual packetized datastreams that constitute a program. These individual streams are termed elementary streams in the

MPEG standard. Elementary streams include datastreams such as video, audio for various languages and caption datastreams. The PAT associates a program number with the PIDs that permit identification and assembly of the packets comprising the PMT. The NIT is optional and may be structured and used to define physical network parameters such as satellite transmission channel frequencies and transponder channels, for example. The CAT contains the conditional access information such as encryption codes that govern access to programs that are dependent upon user entitlement") [column 6 lines 61-67 & column 7 lines 1-13].

- "determining, during replay, whether replay will access encrypted data in the part pointed at by a particular pointer in said list" (i.e. "Units 45 and 47 employ PID detection filters that match the PIDs of incoming packets provided by mux 37 with PID values pre-loaded in control registers within units 45 and 47 by controller 115. The pre-loaded PIDs are used in units 47 and 45 to identify the data packets that are to be stored and the data packets that are to be decoded for use in providing a video image. The pre-loaded PIDs are stored in look-up tables in units 45 and 47. The PID look-up tables are memory mapped to encryption key tables in units 45 and 47 that associate encryption keys with each pre-loaded PID. The memory mapped PID and encryption key look-up tables permit units 45 and 47 to match encrypted packets containing a pre-loaded PID with associated encryption keys that permit their decryption. Non-encrypted packets do not have associated encryption keys. Units 45 and 47 provide both identified packets and their associated encryption keys to decryptor 50. The PID look-up table in unit 45 is also memory mapped to a destination table that matches packets containing pre-loaded PIDs with corresponding destination buffer locations in packet buffer 60. The encryption keys and destination buffer location addresses associated with the programs selected by a user for viewing or storage are pre-loaded into units 45 and 47 along with the assigned PIDs by controller 115. The encryption keys are generated by ISO 7816-3 compliant smart card system 130 from encryption codes extracted from the input datastream. The generation of the encryption keys is subject to customer entitlement determined from coded information pre-stored on the insertable smart card itself (International Standards Organization document ISO 7816-3 of 1989 defines the interface and signal structures for a smart card system)") [column 4 lines 59-67 & column 5 lines 1-22].

- "upon said determining using the list to supply decryption information from the item associated with the particular pointer" (i.e. "Units 45 and 47 employ PID detection filters that match the PIDs of incoming packets provided by mux 37 with PID values pre-loaded in control registers within units 45 and 47 by controller 115. The pre-loaded PIDs are used in units 47 and 45 to identify the data packets that are to be stored and the data packets that are to be decoded for use in providing a video image. The pre-loaded PIDs are stored in look-up tables in units 45 and 47. The PID look-up tables are memory mapped to encryption key tables in units 45 and 47 that associate encryption keys with each pre-loaded PID. The memory mapped PID and encryption key look-up tables permit units 45 and 47 to match encrypted packets containing a pre-loaded PID with associated encryption keys that permit their decryption. Non-encrypted packets do not have associated encryption keys. Units 45 and 47 provide both identified packets and their associated encryption keys to decryptor 50. The PID look-up table in unit 45 is also memory mapped to a destination table that matches packets containing pre-loaded PIDs with corresponding destination buffer locations in packet buffer 60. The encryption keys and destination buffer location addresses associated with the programs selected by a user for viewing or storage are pre-loaded into units 45 and 47 along with the assigned PIDs by controller 115. The encryption keys are generated by ISO 7816-3 compliant smart card system 130 from encryption codes extracted from the input datastream. The generation of the encryption keys is subject to customer entitlement determined from coded information pre-stored on the insertable smart card itself (International Standards Organization document ISO 7816-3 of 1989 defines the interface and signal structures for a smart card system)") [column 4 lines 59-67 & column 5 lines 1-22].

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 5 & 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Blatter.

Claim 5:

Blatter discloses a method of processing an incoming data stream that contains a stream of encrypted data and a stream of messages, data in successive segments of the stream of encrypted data being decryptable with successive decryption information from the messages, as in Claim 1 above, but does not explicitly disclose,

- "constructing a list of data pointers to selected parts of the stream of encrypted data that contain image frames, each data pointer being associated with a selected one of the items of decryption information that enables decryption of the encrypted data pointed at by the pointer"
- "selecting, during replay, the parts of the stream pointed at by pointers in the list"
- "using the list to supply decryption information from the item associated with each pointer"

however, Blatter does disclose,

- "Control unit 65 determines a series of read and write pointers associated with packets stored in buffer 60 based on the First-In-First-Out (FIFO) principle. The write pointers in conjunction with the destination flags permit sequential storage of an identified packet from units 45 or 50 in the next empty location within the appropriate destination buffer in unit 60. The read pointers permit sequential reading of packets from the appropriate unit 60 destination buffers by controller 115 and application interface" [column 5 lines 47-56];
- "The read pointers permit sequential reading of packets from the appropriate unit 60 destination buffers by controller 115 and application interface" [];
- "The PID look-up table in unit 45 is also memory mapped to a destination table that matches packets containing pre-loaded PIDs with corresponding destination buffer

> locations in packet buffer 60. The encryption keys and destination buffer location addresses associated with the programs selected by a user for viewing or storage are pre-loaded into units 45 and 47 along with the assigned PIDs by controller" [column 5 lines 8-15].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to include, "constructing a list of data pointers to selected parts of the stream of encrypted data that contain image frames, each data pointer being associated with a selected one of the items of decryption information that enables decryption of the encrypted data pointed at by the pointer" and "selecting, during replay, the parts of the stream pointed at by pointers in the list" and "using the list to supply decryption information from the item associated with each pointer," in the invention as disclosed by Blatter since the use of pointers to reference and track locations of information are commonly used in conjunction with tables (i.e. lists).

Claim 6:

Blatter discloses a method of processing an incoming data stream that contains a stream of encrypted data and a stream of messages, data in successive segments of the stream of encrypted data being decryptable with successive decryption information from the messages, as in Claim 1 above, but does not explicitly disclose,

- "decrypting item of decryption info from incoming data stream"
- "re-encrypting items of decrypted info with recorded key prior to storage"
- "storing re-encrypted items of decryption info separately from encrypted data stream"

however, Blatter does disclose,

- "The stored encryption code is recovered in a subsequent program retrieval operation and is used to generate an encryption key permitting decryption of the encrypted program for display" [column 9 lines 50-53];
- "The encryption key may only be generated from the recovered code if permitted by entitlement data pre-stored on an insertable smart card in the manner previously discussed" [column 9 lines 53-56];
- "The elementary streams that comprise the individual programs to be stored are determined by controller 115 from the previously stored PSI data. In step 320, controller 115 determines from the user input data SE provided via interface unit 120 (FIG. 1) whether or not individual programs are to be stored in encrypted form" [column 9 lines 41-44];

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to include, "decrypting item of decryption info from incoming data stream" and "re-encrypting items of decrypted info with recorded key prior to storage" and "storing re-encrypted items of decryption info separately from encrypted data stream," in the invention as disclosed by Blatter since encryption keys can be used to decrypt encrypted data. It is obvious that an encryption key may be used to re-encrypt (i.e. or just plain encrypt) data if it is permitted by entitlement data, hence one of its purposes. It is also implied that if individual programs are comprised of streams and their storage is determined based on a criteria, that encrypted information would be stored separately from other data.

5. Claims 7 & 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Heer et al (US-6028933-A).

Claim 7:

Heer et al disclose an apparatus processing an incoming data stream that contains a stream of encrypted data and a stream of messages, data in successive segments of the stream of encrypted data being decryptable with successive decryption information from the messages, but do not explicitly disclose,

- "a storage device"
- "a demultiplexer writing the stream of encrypted data to the storage device"
- "a decryption information recording unit writing items with decryption information from the stream of messages to the storage device"
- "further writing to the storage device synchronization information linking respective points in the stored stream of encrypted data to respective ones of the items with decryption information"
- "a control unit replaying a stored part of the stream of encrypted data"
- "wherein during said replaying a part of the encrypted data and corresponding items with decryption information are retrieved from the storage device according to the synchronization information"

however, Heer et al do disclose,

- "stored in NVM" [column 31 lines 25-26];

- "The demultiplexer 260 removes the PF 263, the FCF 262, and any idle PDUs 261 which may have been included in the transmission. The remainder of the received data stream is sent through a decryptor 270 to remove the ADAPT header and decrypt the encrypted data Various payload components are separated and processed, as will be described later in greater detail" [column 8 lines 30-35];
- "The HE decrypts the message and decrypts E.sub.SSKauth [SN] that it had previously received to authenticate the CM, HE and CM then store PMK in NVM and both also have a shared secret key and so may commence with a connection" [column 31 lines 6-10];
- "Cryptosync is defined as the process of synchronizing an encryption algorithm at a transmitter with a decryption algorithm at a receiver" [column 36 lines 23-25];
- "Some of the envisioned applications include Internet access, the ability to communicate with the office while working at home, voice and video telephony, interactive game playing, etc" [column 1 lines 47-50];
- "Cryptosync is defined as the process of synchronizing an encryption algorithm at a transmitter with a decryption algorithm at a receiver" [column 36 lines 23-25];

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to include, "a storage device" and "a demultiplexer writing the stream of encrypted data to the storage device" and "a decryption information recording unit writing items with decryption information from the stream of messages to the storage device" and "further writing to the storage device synchronization information linking respective points in the stored stream of encrypted data to respective ones of the items with decryption information" and "a control unit replaying a stored part of the stream of encrypted data" and "wherein during said replaying a part of the encrypted data and corresponding items with decryption information are retrieved from the storage device according to the synchronization information," in the invention as disclosed by Heer et al since it is inherent and obvious that the use of storage such as non-volatile memory is commonly used and is necessary for handling of information. The demultiplexer would be "writing the stream of encrypted data to the storage device" when it passes the encrypted data to the decryptor to be decrypted, which implies a necessary storage device in order to hold the encrypted data. The headend (HE) is used to decrypt information and together with the cable modem (CM) store (i.e. write) decryption information from the stream to the storage device. Cryptosync is commonly used for encryption/decryption synchronization in order to reduce data loss due to error rate. Many of the voice and video telephony, interactive game playing, etc require a "control unit" for play and replay of content. Retrieval (i.e. replay) of encrypted content from a storage device would require synchronized retrieval if cryptosync was used for error rate control.

Claim 8:

Heer et al disclose an apparatus processing an incoming data stream that contains a stream of encrypted data and a stream of messages, data in successive segments of the stream of encrypted data being decryptable with successive decryption information from the messages, as in Claim 7 above, further comprising,

- "the items of decryption information are written separately to the storage device to allow access separately from the encrypted data" (i.e. "The remainder of the received data stream is sent through a decryptor 270 to remove the ADAPT header and decrypt the encrypted data Various payload components are separated and processed, as will be described later in greater detail. These payload components include VL PDUs 271, ATM PDUs 272, STM PDUs 274, and control messages 273 carried as VL PDUs") [column 8 lines 33-37];

- "during replay the decryption information is accessed separately from the encrypted data and combined during replay at times selected under control of the synchronization information" (i.e. "The remainder of the received data stream is sent through a decryptor 270 to remove the ADAPT header and decrypt the encrypted data Various payload components are separated and processed, as will be described later in greater detail. These payload components include VL PDUs 271, ATM PDUs 272, STM PDUs 274, and control messages 273 carried as VL PDUs") [column 8 lines 33-37];
- "the items which are combined being selected and/or a time when the items are combined with the stream being selected, dependent on the synchronization information" (i.e. "Cryptosync is defined as the process of synchronizing an encryption algorithm at a transmitter with a decryption algorithm at a receiver") [column 36 lines 23-25].

Response to Arguments

6. Applicant's arguments filed 04/04/2007 have been fully considered but they are not persuasive. Applicant's arguments regarding independent Claim 1 and dependent Claims 2-6 have been considered above in the standing 35 U.S.C. 102(b) and 35 U.S.C. 103(a) rejections and are non-persuasive.

- Applicant argues that Blatter does not disclose "storing items with decryption information from the stream of messages" and "storing the stream of encrypted data." However, it is inherent that decryption information and encrypted data from a stream of messages would be stored on some form of computer readable storage medium, whether it being volatile or non-volatile memory in order for it to be processed.
- Applicant argues that decryption information is different from encrypted packets, and the examiner agrees that these two are different, however, the decryptor would have to have obtained (i.e. storing items with decryption information from the stream of messages) decryption information at some point during the transmission prior to receiving encrypted data for decryption. The applicant never claims which message that the decryption information is a part of.
- The applicant argues that Blatter must decrypt in order to access the adaptation information in order to synchronize, however, the examiner disagrees since the information is located in the packet header and thus need not be decrypted. That is, the timing information permits the synchronizing of encoding and decoding (i.e. encryption/decryption) in order to allow proper decryption while mitigating error rate.

- The applicant argues that Blatter does not disclose coverage for "linking respective points in the stored stream of encrypted data to respective ones of the items with decryption information." However, Blatter does disclose timing information used for the synchronization of encoding/decoding, which implies that the invention, as disclosed by Blatter, links encoding information with decoding information in accordance to specific times. That is, encoding/decoding would not succeed if the timing between two devices were not synchronized.
- The applicant argues that Blatter does not disclose "retrieving the items with decryption information for the points in said stored part during said replaying." The examiner agrees that Blatter does not explicitly disclose this , however, it is inherent that if packets can be identified by their PIDs then the method for handling encrypted and non-encrypted data packets would also apply for decryption packets.
- The applicant argues that CPSI is not equivalent to "replaying a stored part of the stream of encrypted data in an abnormal temporal pattern." The examiner agrees that CPSI is not the same, however, the cited section from Blatter does disclose "a playback device may cross program boundaries during a trick play or search operation." The playback device would "replay" a stored part of the stream, where program boundaries would imply encryption data protecting sections of information, and trick play commonly uses abnormal temporal patterns.

Conclusion

7. Applicant's arguments filed 04/04/2007 have been fully considered but they are not persuasive.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OAL
05/30/2007

Nasser Moazzami
Supervisory Patent Examiner

6/5/07